Zertifizierung gemäß ISO/IEC 27001

datenschutz cert

Einleitung

ISO/IEC 27001 ist der internationale Standard für Informationssicherheit. Er behandelt Anforderungen an ein Informationssicherheits-Managementsystem. Dadurch werden Prozesse in einer Organisation etabliert, um Informationssicherheit dauerhaft zu gewährleisten.

Ob der Standard eingehalten wird, kann von unabhängigen Auditoren überprüft und durch ein ISO/IEC 27001-Zertifikat nach außen dokumentiert werden - etwa um gesetzlichen Anforderungen nachzukommen oder den Erwartungen Ihrer Kunden zu genügen.

Zeigen Sie mit einem Zertifikat nach ISO/IEC 27001, dass die Anforderungen dieser internationalen Norm umgesetzt werden.

Und an dieser Stelle können wir Sie unterstützen: Die datenschutz cert GmbH ist bei der Deutschen Akkreditierungsstelle (DAkkS) akkreditiert. Danach dürfen wir international gültige ISO/IEC 27001-Zertifikate erteilen.

Sprechen Sie uns an. Wir freuen uns auf Sie!

Kai Osterhage

datenschutz cert GmbH
Ihr Ansprechpartner:
Kai Osterhage
+49 (0) 421 69 66 32-556
kosterhage@datenschutz-cert.de

Vorteile Ihres ISO/IEC 27001-Zertifikates

- Erfüllung gesetzlicher Anforderungen, z.B.:
  - IT-Sicherheitsgesetz
  - IT-Sicherheitskatalog
  - TR-03109 / Messstellenbetriebsgesetz
  - KonTraG
  - Energiewirtschaftsgesetz
  - Glücksspielrecht
  - MaRisk
  - Sarbanes-Oxley-Act
- Erfüllung der Erwartung Ihrer Kunden
- Prozessverbesserung und damit Produktivitätssteigerung
- Informationssicherheit
- Datenschutz
- Haftungsreduktion
- Synergien zu anderen Managementprozessen, z.B.:
  - ISO 9001
  - ISO/IEC 20000-1

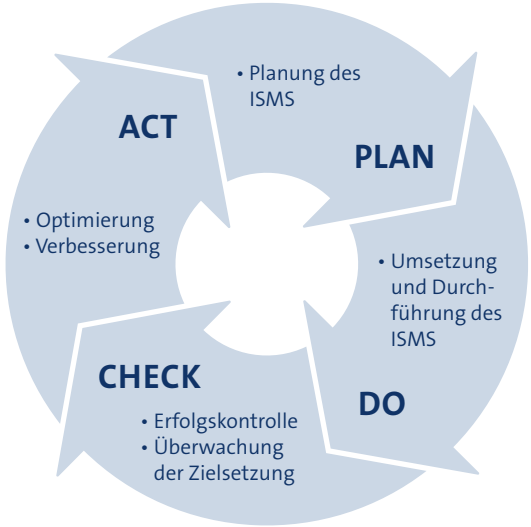
Gesetzliche Vorgaben für KRITIS

Mit dem IT-Sicherheitsgesetz und dem IT-Sicherheitskatalog hat der Gesetzgeber Vorgaben für Betreiber Kritischer Infrastrukturen (KRITIS) und Netzbetreiber erlassen. Hintergrund ist, dass zunehmend IT-Infrastrukturen wichtige Versorgungsbereiche durchdringen. So gewinnt Informationstechnik und deren Sicherheit an Stellenwert – besonders für die wichtige Verfügbarkeit.

Wie sieht ein ISMS aus?

Datenschutz und Informationssicherheit sind zwei zentrale Anforderungen der Informationsgesellschaft. Es hat sich gezeigt, dass für eine ganzheitliche Informationssicherheit eine strukturierte Herangehensweise erforderlich ist – durch ein Informationssicherheits-Managementsystem (ISMS).

Ein ISMS ist ein ganzheitlicher, strukturierter Top-Down-Ansatz, um Informationssicherheit in einer Organisation zu etablieren und effizient und wirkungsvoll umzusetzen. Ein ISMS ist ein „lebender" Prozess, in dem das Management regelmäßig über den Zustand des ISMS informiert wird, wodurch das Management seine Verantwortung wahrnehmen und ggf. reagieren kann. Ein ISMS ist skalierbar und auch für größere Organisationen einsetzbar. Der ISMS-Prozess ist auch bekannt als PDCA-Zyklus: Plan – Do – Check – Act.



Basis für weitere Normen

ISO/IEC 27001 stellt die Basisnorm für weitere branchenspezifische Anforderungen dar, etwa:

- ISO/IEC 27011 für Telekommunikationsunternehmen,
- ISO/IEC 27017 für IT-Sicherheit in der Cloud,
- ISO/IEC 27018 für Datenschutz in der Cloud,
- ISO/IEC 27019 für die Energiewirtschaft,
- ISO 27799 für das Gesundheitswesen,
- TR 03109-6 für Smart Meter Gateway Administration.

Gerne informieren wir Sie, wie diese branchenspezifischen Anforderungen in eine ISO/IEC 27001-Zertifizierung integriert werden können.

Multiple Site: Zertifizierung eines ISMS an mehreren Standorten

Ein Informationssicherheits-Managementsystem kann sich über mehrere Standorte oder sogar juristische Personen verteilen. So ist es möglich, einen kompletten Unternehmensverbund zu zertifizieren und dabei Synergieeffekte sinnvoll zu nutzen. Voraussetzung ist dabei, dass alle Einheiten unter einem zentralen Managementsystem interagieren und gesteuert werden, wobei einzelne Tätigkeiten sich auf die Unternehmenseinheiten verteilen lassen. Durch ein gemeinsames Audit aller Einheiten sparen Sie Zeit und Ressourcen, sowohl bei der Vorbereitung als auch bei der Zertifizierung Ihres ISMS gemäß ISO/IEC 27001.

Sprechen Sie uns gerne an, um konkrete Möglichkeiten zur Durchführung einer Multiple Site-Zertifizierung zu erfahren.

Unabhängige Audits und Zertifizierung

Um Ihnen ein Höchstmaß an Unabhängigkeit zu garantieren, setzen wir auf ein zweistufiges Zertifizierungsverfahren:

1) Der bei der datenschutz cert GmbH lizenzierte Lead-Auditor prüft die Konformität des Informationssicherheits-Managementsystems gemäß ISO/IEC 27001 und empfiehlt im Auditreport die Zertifizierung. Es ist möglich, beim Audit nach ISO/IEC 27001 direkt branchenspezifische Anforderungen mit zu begutachten.

2) Die Zertifizierungsstelle prüft das Auditverfahren, insbesondere um eine Vergleichbarkeit zwischen den Audits sicher zu stellen. Anschließend kann die Zertifizierung ausgesprochen und das Zertifikat erstellt werden.

Aufwand der Auditierung

Der Umfang der Auditierung orientiert sich an der für alle akkreditierten Zertifizierungsstellen bindenden Norm ISO/IEC 27006. Hier werden in Abhängigkeit der Größe des ISMS (Anzahl der Mitarbeiter im Geltungsbereich) folgende Vorgaben genannt.

Anzahl der Mitarbeiter im Geltungsbereich	1 - 10	11 - 25	26 - 45	46 - 65	66 - 85	86 - 125	...
Anzahl der Tage für die Auditierung	5	6	7	8,5	11	12	...

Sprechen Sie uns gerne an!
Wir unterbreiten Ihnen ein konkretes Angebot.

Zertifizierungsprozess

Laufzeit des Zertifikats
(i.d.R. 3 Jahre)

Erst-Zertifizierung

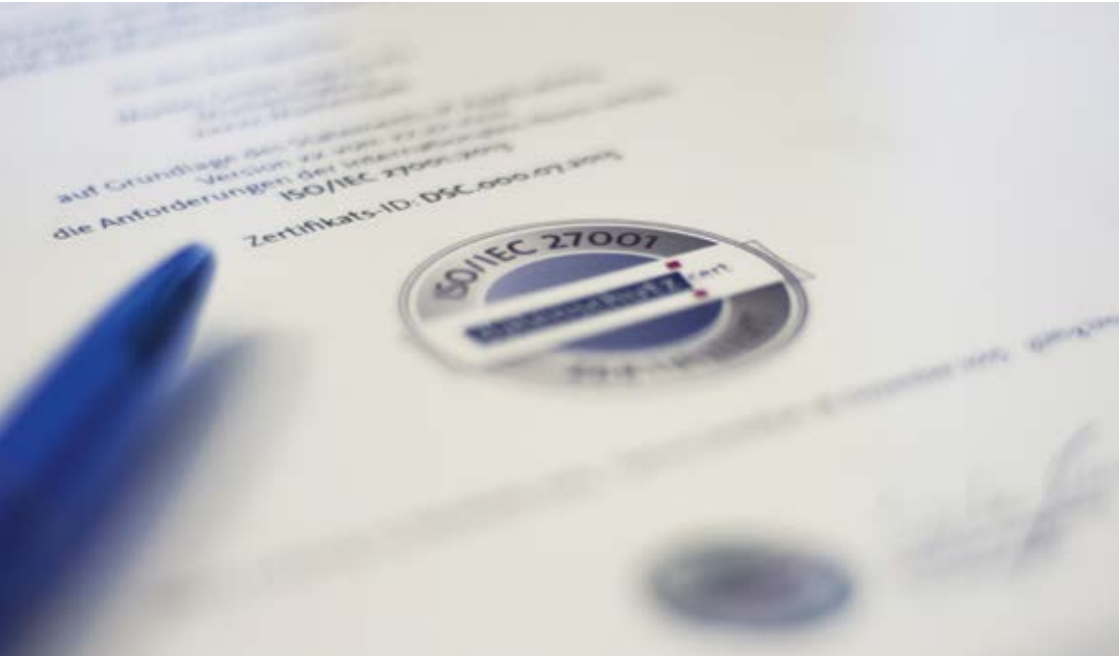
- Auditierung
  - Vorbereitung/Sichtung Referenzdokumente
  - Preaudit
  - Audit
  - ausführlicher Report
- Zertifizierung
  - Zertifizierungstätigkeit
  - Ausstellung Zertifikat
  - Übergabe des Zertifikats
  - Listung im Internet über gesamte Laufzeit

1. Überwachungsaudit (nach einem Jahr)

2. Überwachungsaudit (nach zwei Jahren)

Re-Zertifizierung

- Auditierung
- Zertifizierung



datenschutz cert GmbH

Hauptsitz Bremen
Konsul-Smidt-Straße 88a
28217 Bremen

Niederlassung Berlin-Mitte
Reinhardtstraße 46
10117 Berlin

Tel.: 0421 69 66 32 50
office@datenschutz-cert.de
www.datenschutz-cert.de

Wir sind bei der Deutschen Akkreditierungsstelle (DAkkS) als Zertifizierungsstelle akkreditiert.

DAkkS Deutsche Akkreditierungsstelle D-ZM-16077-01-00